REMARKS

To date, the Examiner has not indicated that the subject matter of the information disclosure statement (IDS) filed February 03, 2006 has been properly considered. A copy of such IDS is submitted herewith. If the Examiner requires additional copies of any reference(s), applicant invites the Examiner to contact the undersigned. Documentation in the file wrapper of the instant application confirming the Examiner's consideration of the reference(s) is respectfully requested.

The Examiner has rejected Claim 25 due to informalities. This rejection is deemed moot in view of the clarification made hereinabove to Claim 25.

In addition, the Examiner has rejected Claims 1, 39, and 41 under 35 U.S.C. 112, second paragraph, as being indefinite. Applicant respectfully disagrees with this rejection.

With respect to Claim 1, the Examiner argues that it is unclear whether the claimed identifiers were the same. In response, applicant notes that such claim requires that "the proxy device [be]... assigned the same identifier as is assigned to the file storage device." Further, when there is a plurality of file storage devices, such claim requires that the "proxy device [be] assigned multiple identifiers corresponding to the identifiers of the connected file storage devices" (emphasis added). Since there is nothing in such claim language forbidding the proxy device to be assigned multiple identifiers (such that it is assigned the same identifier as each of those assigned to multiple file storage devices), the claims are clearly definite. If the Examiner would like to discuss such issue further, the undersigned invites a call for such purpose.

With respect to Claim 39, the Examiner has taken issue with the term "associated." Applicant respectfully disagrees with such rejection, as such term is clearly definite, as evidenced by its plain and ordinary meaning. Note, for example, the following illustrative dictionary definition which is consistent with the specification:

associate

Joined with another or others and having equal or nearly equal status
Having partial status or privileges
Following or accompanying

The American Heritage® Dictionary of the English Language, Fourth Edition
Copyright © 2000 by Houghton Mifflin Company.
Published by Houghton Mifflin Company. All rights reserved.

With respect to Claim 41, such rejection is deemed moot in light of the clarification made hereinabove to such claim. Specifically, applicant has deleted the word "minimal" to clarify that which is being claimed by applicant.

The Examiner has rejected Claims 1, 3-9, 12, 13, 15-21, 24, 25, 27-33, 36, and 39-41 under 35 U.S.C. 103(a) as being unpatentable over Tso (U.S. Patent No. 6,088,803) in view of Ceniza (U.S. Publication No. 2002/0186698). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims.

With respect to each of the independent claims, the Examiner has relied on the following excerpts from the Tso to make a prior art showing of applicant's claimed technique "wherein the processing logic is responsive to configuration data to determine which malware scanning algorithms should be selected for a particular file, the proxy device further comprising a scanning engine to execute the malware scanning algorithms selected by the processing logic" (see this or similar, but not necessarily identical language in each of the independent claims).

> "Once the file is completely received, network device 4 invokes virus checker 5, which in turn performs its preconfigured virus scan processing with the requested file as input (Step 40). If the requested file does not contain a virus, network device 4

> transmits the file to client device 1 (Step 70); if a virus is detected, the file will not be sent and, optionally, network device 4 transmits an appropriate error/warning message to client device 1 and/or content server 7 (Step 60)." (Tso, Col. 3, lines 2-10 - emphasis added)

Applicant respectfully asserts that the excerpt from Tso relied upon by the Examiner teaches a method of performing "preconfigured virus scan processing" at the network device 4 for files being requested by the client device. However, applicant claims the use of "...processing logic [which] is responsive to configuration data to determine which malware scanning algorithms should be selected for a particular file..." Furthermore, once determined by the processing logic, "...the proxy device further compris[es] a scanning engine to execute the malware scanning algorithms selected by the processing logic" (emphasis added). The preconfigured virus scan processing taught by Tso thus simply fails to disclose the technique of "processing logic ... to determine which malware scanning algorithms should be selected for a particular file," as claimed by applicant.

It appears from the Examiner's "Response to Arguments, that the Examiner has relied on an inherency argument regarding the above emphasized claim limitations. In view of the arguments made hereinabove, any such inherency argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112)

Still yet, the Examiner has relied on the following excerpts from Ceniza to make a prior art showing of applicant's claimed technique "wherein each device in the computer network is assigned an identifier, and the proxy device is assigned the same identifier as is assigned to the file storage device, the first interface being connectable to a communication infrastructure of the computer network to enable communication between the proxy device and said client devices, and the file storage device being connectable to the second interface such that the file storage device is only accessible by said client

devices via said proxy device" (see this or similar, but not necessarily identical language in each of the independent claims).

> "[0043] As shown in FIG. 4, each host on Networks "B.", "C," and "D" has been assigned a virtual IP address by which it can be referenced from Network "A." FIG. 4 also shows that the virtual addresses assigned to Network "D" are the same as the actual local IP addresses for that network. As a general rule, where remote networks are to be incorporated into the internetwork design of this invention, local IP addresses should be assigned to correspond with the virtual IP addresses for that network unless other considerations (such as a desire to maintain an earlier addressing scheme, or the need to maintain compatibility with other parts of a pre-existing LAN) outweigh that choice." (Ceniza, Paragraph 0043 - emphasis added)

Applicant respectfully asserts that the above excerpt from Ceniza relied upon by the Examiner teaches a method of incorporating remote networks into a local LAN by use of virtual IP addresses. Specifically, Ceniza teaches the technique where 'each host on Networks "B.", "C," and "D" has been assigned a virtual IP address by which it can be referenced from Network "A".' Such excerpt from Ceniza fails, however, to even mention the use of a "proxy device [that] is assigned the same identifier as is assigned to the file storage device" (emphasis added), as claimed. Furthermore, such excerpt from Ceniza fails to even suggest a technique where "the file storage device being connectable to the second interface such that the file storage device is only accessible by said client devices via said proxy device" (emphasis added), as claimed.

Ceniza teaches that virtual IP addresses allow Network "A" to reference hosts on networks "B," "C," or "D" directly. Clearly, Ceniza's disclosure of the use of virtual IP addresses to connect multiple networks fails to even suggest a technique "wherein each device in the computer network is assigned an identifier, and the proxy device is assigned the same identifier as is assigned to the file storage device ... such that the file storage device is only accessible by said client devices via said proxy device" (emphasis added), as claimed by applicant.

Even still, the Examiner has relied on the following excerpts from Ceniza to make a prior art showing of applicant's claimed technique "wherein the second interface is

configured to enable a plurality of file storage devices to be connected to the proxy device, each file storage device having a different identifier, and the proxy device being assigned multiple identifiers corresponding to the identifiers of the connected file storage devices, the first interface being configured to receive any access requests issued to one of said connected file storage devices" (see this or similar, but not necessarily identical language in each of the independent claims).

> "[0042] FIG. 4 shows the overall network address scheme. Actual hosts on Network "A" 10 have the actual IP addresses listed for that network. Actual IP addresses for Networks "B" 70, "C" 120, and "D" 170 are listed under "Actual LAN IP Addresses." Virtual addresses for those networks and the hosts attached to them, as seen from Network "A" are listed under "Virtual LAN IP Addresses on Network A." Virtual IP addresses of the hosts on Network "A," as seen locally from the other networks are listed under "Virtual LAN IP Addresses on Local LAN." The global IP addresses of the VPN-routers are listed under "Internet IP Addresses (Global)." Each host on each network has been designated by a number (Host 1, Host 2, etc. . . .) for ease of reference. The host numbers, however, are simply illustrative references, and have nothing to do with the addressing scheme of this invention." (Ceniza, Paragraph 0042 - emphasis added)

Applicant respectfully asserts that the above excerpt from Ceniza relied upon by the Examiner merely teaches that each network host has a virtual and actual IP address where the virtual IP address is visible from other networks. Specifically, Ceniza discloses where the '[a]ctual hosts on Network "A" 10 have the actual IP addresses listed for that network' (emphasis added) and '...Virtual IP addresses of the hosts on Network "A," [are] seen locally from the other networks...' However, the above excerpt from Ceniza fails to even mention a technique "wherein ... the proxy device [is] being assigned multiple identifiers corresponding to the identifiers of the connected file storage devices..." (emphasis added), as claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined)

must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has amended each of the independent claims to further distinguish applicant's claim language from the above reference, by incorporating the subject matter of Claim 10 and 43 et al. as follows:

> "wherein, upon receipt of an access request from a client device, the processing logic is arranged to determine from the access request predetermined attributes, and to send those predetermined attributes to the file storage device to enable the file storage device to perform a validation check, the processing logic only allowing the access request to proceed if the file storage device confirms that the client device is allowed to access the file identified by the file access request;
>
> wherein the plurality of client devices are allowed direct access to the file storage device if the proxy device fails" (see this or similar, but not necessarily identical language in the independent claims).

With respect to the subject matter of former Claim 10 et al. (now at least substantially incorporated into the independent claims), the Examiner has rejected the same under 35 U.S.C. 103(a) as being unpatentable over Tso in view of Ceniza in view of Cuomo (U.S. Publication No. 2002/0091757). Specifically, the Examiner has relied on the following excerpt from Cuomo to make a prior art showing of applicant's claimed technique "wherein, upon receipt of an access request from a client device, the processing logic is arranged to determine from the access request predetermined attributes, and to send those predetermined attributes to the file storage device to enable the file storage

device to perform a validation check, the processing logic only allowing the access request to proceed if the file storage device confirms that the client device is allowed to access the file identified by the file access request" (see this or similar, but not necessarily identical language in the independent claims).

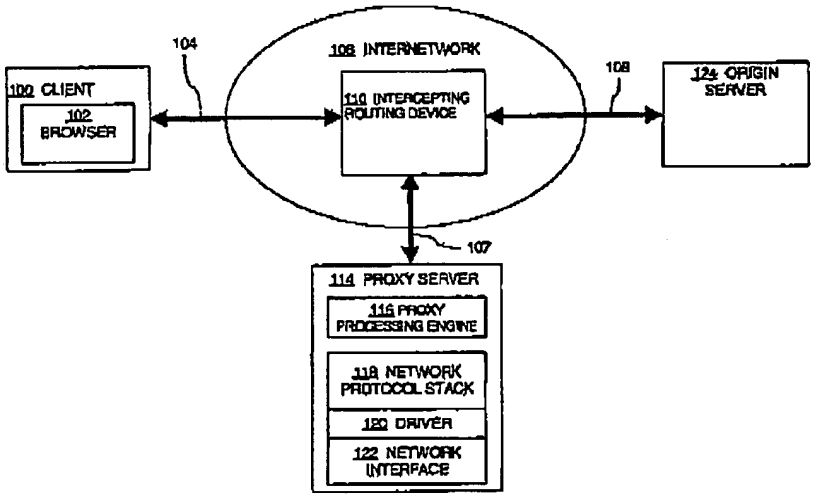
> "Through applets and Web pages, users generate requests to access resources on the Web. Reverse Proxy servers may be used to act as a gateway into an Intranet environment. The users trying to access a resource will make requests to a reverse proxy server which would forward the request to a backend server that processes that particular requests. **It is common for using these reverse proxy servers for authentication purposes as well.** In other words, these servers make sure that users are who they say they are in a request This authentication may take many different forms, including the use of user IDs and passwords. **Before forwarding this request to the backend server, the reverse proxy server might include and/or modify information on the authenticated user's identity.** This may be in the form of a header, a credential token or in some other authentication data format. **Thereafter, authenticated requests are sent to backend services for processing.** The present invention recognizes that most backend services do not understand or recognize credential information that might be passed along with or within a request from a reverse proxy server. **It also recognizes the fact that the backend server must trust the reverse proxy server in order to accept and work with the forwarded request."** (Cuomo, Paragraph 0007 - emphasis added)

Applicant respectfully asserts that the above excerpt from Cuomo referenced by the Examiner teaches that it is "... common [to] us[e] these reverse proxy servers for authentication purposes ..." The reverse proxy server sends "authenticated requests ... to backend services for processing" (emphasis added). Cuomo also discloses that the "backend server must trust the reverse proxy server in order to accept and work with the forwarded request" (emphasis added). However, this method contrasts with applicant's claimed technique wherein "the processing logic is arranged to determine from the access request predetermined attributes to send those predetermined attributes to the file storage device to enable the file storage device to perform a validation check" (emphasis added), as claimed.

With respect to the subject matter of former Claim 43 (now at least substantially incorporated into the independent claims), the Examiner has rejected the same under 35

U.S.C. 103(a) as being unpatentable over Tso in view of Ceniza in view of Bector (U.S. Patent No. 6,687,732). In particular, the Examiner has relied on the following excerpt from Bector to make a prior art showing of applicant's claimed technique "wherein the plurality of client devices are allowed direct access to the file storage device if the proxy device fails."

> 'If the driver 120 fails to receive a "heartbeat" message over a pre-determined interval of time, the driver assumes that the proxy processing engine 116 is unavailable or has crashed. In response, driver 120 causes all traffic to be bypassed until the proxy processing engine 116 comes back on-line. The driver may also monitor system resources, such as process identifiers, process semaphores, and open connections to detect system failure. Additionally, if the proxy server has failed repeatedly several times in close proximity, the driver will persistently bypass traffic away from the proxy server, even after heartbeats resume, as a fail-safe measure so a failing proxy server will not cause the system to "flap".' (Bector, Col. 13, lines 55-67 - emphasis added)



(Bector, Figure 1, not specifically cited)

Applicant respectfully asserts that the excerpt from Bector referenced by the Examiner simply teaches a technique where a driver 120 of a proxy server 114 bypasses traffic when a proxy processing engine 116 of the proxy server fails. Specifically, the "driver 120 causes all traffic to be bypassed until the proxy processing engine 116 comes back on-line" (emphasis added). Bector, however, fails to even suggest actions taken

when the proxy server 114 fails and simply discloses that "the driver will persistently bypass traffic away from the proxy server" (emphasis added). There is thus simply no disclosure in such excerpt where "...the plurality of client devices are allowed direct access to the file storage device if the proxy device fails" (emphasis added), as claimed by applicant.

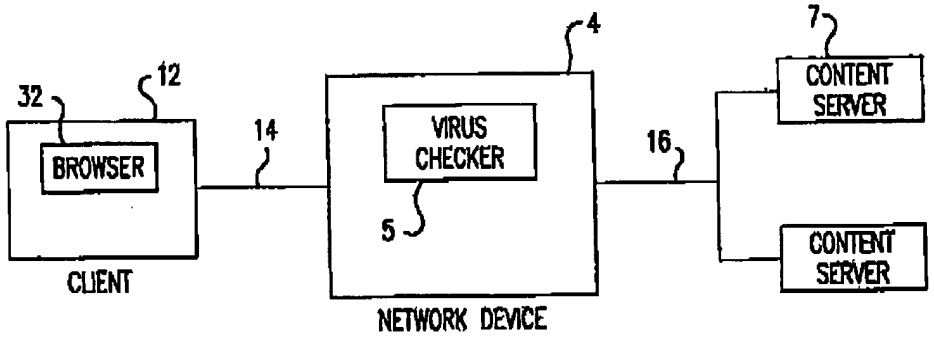
Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to dependent Claims 9, 21, and 33, the Examiner has relied on the following excerpt from Tso to make a prior art showing of applicant's claimed technique "wherein the file cache is arranged only to store files which have been determined not to be considered as malware."

> "Referring now to FIG. 4, since virus checking can be a resource-intensive operation, checked files and/or results of checks may be advantageously stored in a cache storage 30 resident in, or coupled to, network device 4. Future requests for the same data object may then be serviced immediately without having to recheck the file. Network device 4 may also include a cache interface 28 configured to check whether a cached object has been updated on content server 7 since being cached, in which case network device 4 will retrieve the updated file and initiate virus checking as described above. If the virus repairing option is implemented, the repaired data object may be stored in cache storage 30." (Tso, Col. 5, lines 1-13 - emphasis added)

Applicant respectfully asserts that the above excerpt from Tso relied upon by the Examiner teaches a technique where "checked files and/or results of checks may be advantageously stored in a cache storage" (emphasis added) so that "[f]uture requests for the same data object may then be serviced immediately without having to recheck the file." There is simply no disclosure in such Tso excerpt, however, of a technique to "only to store files which have been determined not to be considered as malware" (emphasis added), as claimed by applicant.

In addition, with respect to dependent Claim 39, the Examiner has relied on the following figure from Tso to make a prior art showing of applicant's claimed technique "wherein for a plurality of file storage devices on the computer network, a plurality of

proxy devices are provided such that each file storage device is associated with one of the proxy devices."



(Tso, Fig. 1, note cited)

"Embodiments of the present invention are directed to a system for virus checking network data to be downloaded to a client device, such as data retrieved from an Internet content server in response to a browser request. With reference to FIG. 1, according to a first embodiment of the present invention a client device 12 may access a plurality of content servers 7 through a network device 4. Content servers 7 may reside, for example, on the Internet; however, the present invention is not limited to any particular network or networking environment." (Tso, Col. 2, lines 16-25 - emphasis added)

Applicant respectfully asserts that the figure and excerpt from Tso relied upon by the Examiner discloses a technique where "a client device 12 may access a plurality of content servers 7 through a network device 4" (emphasis added). However, "access[ing] a plurality of content servers ... through a network device" simply does not imply a technique where "each file storage device is associated with one of the proxy devices" (emphasis added), as claimed by applicant.

Also, with respect to dependent Claim 41, the Examiner has relied on the following excerpt from Tso to make a prior art showing of applicant's claimed technique "wherein the proxy device is associated with all of the file storage devices when ... scanning of files is performed.

"Given the availability of new virus patterns which have not been used to scan these cached files, network device 4 may simply

> expire all of the cached objects to avoid the possibility that a now-known virus was missed." (Tso, Col. 5, lines 19-23 - emphasis added).

Applicant respectfully asserts that the excerpt from Tso relied upon by the Examiner merely teaches that the "network device 4 may simply expire all of the cached objects" (emphasis added) when there are "...new virus patterns which have not been used to scan these cached files." The Tso excerpt above in no way, however, even suggests a technique "wherein the proxy device is associated with all of the file storage devices when ... scanning of files is performed" (emphasis added), as claimed by applicant.

In addition, with respect to the subject matter of Claims 12, 24, and 36, the Examiner has relied on the following excerpt from Gardner to make a prior art showing of applicant's claimed " passive load balancing mechanism arranged to configure each client device to communicate with a particular proxy device in said plurality, such that an access request issued by a particular client device will be directed to a predetermined one of said proxy devices dependent on how that client device was configured by the passive load balancing mechanism."

> "Next, in step S502 of FIG. 5, the blocks in each media server may be allocated in proportion to the bandwidth availability of each first-level I/O device, in order to balance the bandwidth load upon data retrieval. For the configuration shown in FIG. 4A, the first-level I/O devices am the disk controllers a1 and a2. Beginning with disk controllers a1 and a2, although the availability of the controllers as a group is 9.0 MB/sec, each controller has a different bandwidth availability. Controller a1 has an availability of 4.0 MB/sec, while controller a2 has an availability of 5.0 MB/sec. Therefore, the 15,625 file data blocks allocated to media server MS1 will be further allocated between these two controllers according to their bandwidth availability as follows:" (Gardner, Col. 10, lines 55-65 - emphasis added)

Applicant respectfully asserts that the excerpt from Gardner relied upon by the Examiner fails to meet all of applicant's claimed language. Specifically, the above excerpt discloses the technique where "the blocks in each media server may be allocated in proportion to the bandwidth availability of each first-level I/O device, in order to

balance the bandwidth load upon data retrieval" (emphasis added). Splitting a proportion of the blocks between the I/O devices clearly fails to teach the use of "a passive load balancing mechanism arranged to configure each client device to communicate with a particular proxy device in said plurality, such that an access request issued by a particular client device will be directed to a predetermined one of said proxy devices dependent on how that client device was configured by the passive load balancing mechanism", as claimed by applicant.

Moreover, with respect to dependent Claim 38, the Examiner has relied on the following excerpt from Ji to make a prior art showing of applicant's claimed technique "wherein the determination is made according to additional configuration data specifying when scanning should be performed and the types of files that should be scanned."

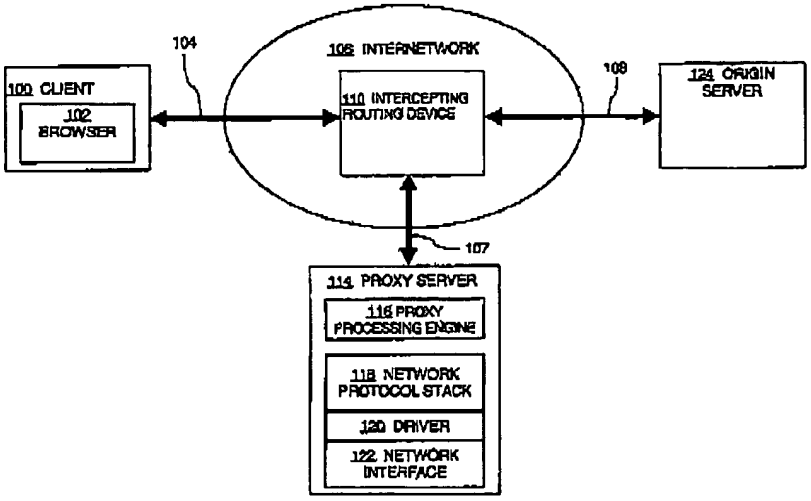
> "If the data is being transferred in an outbound direction, then the method transitions from step 608 to step 610. Referring now to FIG. 6B in conjunction with FIG. 5A, the process for transferring data out of the protected domain of the network is described in more detail. In step 610, the FTP proxy server 60 determines whether the file to be transferred is of a type that can contain viruses. This step is preferably performed by checking the extension of the file name. For example, .txt, .bmd, .pcx and .gif extension files indicate that the file is not likely to contain viruses while .exe, .zip, and .com extension files are of the type that often contain viruses. If the file to be transferred is not of a type that can contain viruses, then the method continues in step 612. In step 612, a second data port 80 is established and the data transfer request & the file are sent from the FTP proxy server 60 to the FTP daemon 78 so that the file can be sent to the server task 82. The FTP daemon 78 is a program executed by the gateway node 33 that communicates the transfer commands to the server task 82, establishes a third port 84 for sending the file including binding the server task 82 and FTP daemon 78 to the third port 84, and transmits the file to the server task 82. Once transmitted, the method is complete and ends. However, if it is determined in step 610 that the file to be transferred is of a type that can contain viruses, the method proceeds to step 614. In step 614, the FTP proxy server 60 transfers the file from the client to the FTP proxy server 60 through the first port 76, and in step 616, the file is temporarily stored at the gateway node 33. Then in step 618, the temporarily stored file is analyzed to determine if it contains viruses. This is preferably done by invoking a virus-checking program on the temporarily stored file. For example, a program the performs a version of signature scanning virus detection such as PC-Cillin manufactured and sold by Trend Micro Devices Incorporated of Cupertino, Calif. may be used. However, those

> skilled in the art will realize that various other virus detection methods may also be used in step 618." (Ji, Col. 7, lines 30-65 - emphasis added)

Applicant respectfully asserts that the excerpt from Ji referenced by the Examiner teaches "the FTP proxy server 60 determines whether the file to be transferred is of a type that can contain viruses [which is] preferably performed by checking the extension of the file name" (emphasis added). The excerpt from Ji continues to teach that the ".txt, .bmd, .pcx and .gif extension files indicate that the file is not likely to contain viruses while .exe, .zip, and .com extension files are of the type that often contain viruses" (emphasis added). However, such excerpt from Ji does not disclose where "additional configuration data specif[ies] when scanning should be performed" (emphasis added), as claimed by applicant. Thus, such excerpt fails to disclose a technique where "the determination is made according to additional configuration data specifying when scanning should be performed and the types of files that should be scanned" (emphasis added), as claimed by applicant.

Furthermore, with respect to dependent Claim 42, the Examiner has relied on the following excerpt from Bector to make a prior art showing of applicant's claimed technique "wherein a computer network administrator has direct access to the file storage device."

> 'If the driver 120 fails to receive a "heartbeat" message over a pre-determined interval of time, the driver assumes that the proxy processing engine 116 is unavailable or has crashed. In response, driver 120 causes all traffic to be bypassed until the proxy processing engine 116 comes back on-line. The driver may also monitor system resources, such as process identifiers, process semaphores, and open connections to detect system failure. Additionally, if the proxy server has failed repeatedly several times in close proximity, the driver will persistently bypass traffic away from the proxy server, even after heartbeats resume, as a fail-safe measure so a failing proxy server will not cause the system to "flap".' (Bector, Col. 13, lines 55-67 - emphasis added)



(Bector, Figure 1, note cited)

Applicant respectfully asserts that the excerpt from Bector referenced by the Examiner teaches a technique where a driver 120 of a proxy server 114 bypasses traffic when a proxy processing engine 116 of the proxy server fails. Specifically, the "driver 120 causes all traffic to be bypassed until the proxy processing engine 116 comes back on-line" (emphasis added). The above excerpt from Bector, however, fails to even mention the technique "wherein a computer network administrator has direct access to the file storage device" (emphasis added), as claimed by applicant.

Still yet, with respect to dependent Claim 44, the Examiner has relied on the following excerpt from Rao to make a prior art showing of applicant's claimed technique "wherein the predetermined attributes include a user name, a password of the user making the access request, a domain of the client device, an indication of the file to be accessed and an address of the client device."

> "That is, once an access protocol becomes available, it is possible to access resources provided by a server using the protocol without regard to the machine type or the operating system of the server." (Rao, Col. 5, lines 60-63 - emphasis added)

Applicant respectfully asserts that the excerpt from Rao relied upon by the Examiner merely teaches the technique where "it is possible to access resources provided

by a server using the protocol" (emphasis added). The excerpt in no way even suggests a technique "wherein the predetermined attributes include a user name, a password of the user making the access request, a domain of the client device, an indication of the file to be accessed and an address of the client device" (emphasis added), as claimed by applicant.

Again, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

To this end, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P453/01.123.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100

RECEIVED
CENTRAL FAX CENTER
APR 13 2006

COPY
PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)
Wolff et al.	) Art Unit: 2134
Application No. 10/003,265	) Examiner: Brown, Christopher J.
Filed: December 06, 2001	) Date: February 3, 2006
For: TECHNIQUES FOR PERFORMING MALWARE SCANNING OF FILES STORED WITHIN A FILE STORAGE DEVICE OF A COMPUTER NETWORK	)

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Commissioner of Patents, Alexandria, VA 22313-1450 on the date noted above.

Signed: _____
Erica L. Farlow

INFORMATION DISCLOSURE STATEMENT
UNDER 37 CFR §§ 1.56 AND 1.97(c)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The reference(s) listed in the attached PTO Form 1449, cop(ies) of which is attached (when necessary), may be material to examination of the above-identified patent application. Applicants submit the reference(s) in compliance with their duty of disclosure pursuant to 37 CFR §§ 1.56 and 1.97. The Examiner is requested to make the reference(s) of official record in this application.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that the reference(s) indeed constitutes prior art.

This Information Disclosure Statement is being filed after the mailing date of a first Office Action. Accordingly, applicants are including payment in the amount of $180.00 for the fee due in connection with the filing of this Information Disclosure Statement. However, if it is determined that any additional fees are due, the Commissioner is hereby authorized to charge such fees or credit any overpayment to Deposit Account 50-1351 (Order No. NAI1P453).

Respectfully submitted,
Zilka-Kotab, PC

Kevin J. Zilka
Reg. No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
Telephone: (408) 971-2573

Form 1449 (Modified) **Information Disclosure Statement By Applicant** (Use Several Sheets if Necessary)	Atty. Docket No. NAI1P453/01.123.01 Applicant: D. Wolff et al. Filing Date: 12/06/2001	Application No.: 10/003,265 Group Art Unit: 2134

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A						
	B						
	C						
	D						
	E						
	F						
	G						
	H						
	I						
	J						
	K						

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation Yes	Translation No
	L							
	M							
	N							
	O							
	P							

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication
	R	Copy of Advisory Action from US Application No. 10/004,120 mailed 11/16/2005.
	S	
	T	

Examiner	Date Considered

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.